Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1, 3-6, 8-12, 15 and 16 are pending in the application, with claims 1, 6, 11 and 12 being the independent claims. Claims 2, 7, 130 and 14 were previously canceled.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Amendment to the Specification

The specification is sought to be amended to correct informalities in the "CROSS-REFERENCE TO RELATED APPLICATIONS" section and to correct typographical errors in paragraphs [0016], [0032], [0051] and [0052]. These changes are believed to introduce no new matter, and their entry is respectfully requested

Rejections under 35 U.S.C. § 103

The Examiner has maintained the rejection of claims 1, 3-6, 8-10, 12, 15 and 16 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,438,123 to Chapman ("Chapman") in view of U.S. Patent No. 6,732,179 to Brown *et al.* ("Brown"). The Examiner has also maintained the rejection of claim 11 under 35 U.S.C. § 103(a) as being unpatentable over Chapman in view of U.S. Patent No. 6,510,162 to Fijolek *et al.* ("Fijolek").

Independent claim 1 recites the following features:

> A cable modem system for transferring data from a user device to a network, comprising:
>
> a cable modem;
>
> a DOCSIS-compliant cable modem termination system coupled to said cable modem via a cable network; and
>
> a headend server coupled to said cable modem termination system and to the network;
>
> wherein said cable modem is adapted to receive data packets from the user device, to modify the contents of said data packets in accordance with a non-DOCSIS-compliant data transfer protocol, to append address information corresponding to said headend server to said modified data packets, and to transfer said modified data packets to said cable modem termination system;
>
> wherein said cable modem termination system is adapted to receive said modified data packets and to transfer said modified data packets to said headend server in accordance with said address information; and
>
> wherein said headend server is adapted to restore the contents of said modified data packets to an unmodified state and to transfer said restored data packets to the network.

Like claim 1, claims 6 and 12 each include a headend server adapted to receive from a CMTS data packets modified in accordance with a non-DOCSIS-compliant data transfer protocol, restore the contents of the modified data packets to an unmodified state, and transfer the restored data packets to a network. Claim 11 recites a similar feature except that the headend server is adapted to transfer the restored data packets back to the CMTS, which then transfers the restored data packets to the network.

The bases for the Examiner's rejection of independent claims 1, 6, 11 and 12 in the instant Office Action are identical to those set forth in the previous Office

Action mailed October 20, 2004. The Examiner has again conceded that Chapman does not disclose the relevant feature of "a headend server that receives the suppressed packets from the CMTS and restores the packets before transmission to a destination." (Office Action mailed June 1, 2005, pages 3 and 6). Thus, the Examiner has again relied upon Brown and Fijolek to disclose this feature. In the instant Office Action, the Examiner has added the following summary of the reasons for rejection with respect to Brown and Fijolek:

> The systems of Brown and Fijolek introduce the concept that a CMTS may operate in conjunction with a server to optimize system performance, add enhanced security features, etc. prior to data transmission over a network. The combination of Chapman and Brown and/or the combination of Chapman and Fijolek suggest that the operation of restoring suppressed packet headers in Chapman could be performed at a headend server cooperating with the CMTS, as shown by Brown and Fijolek, rather than directly at the CMTS, to enable system optimization and enhanced services to [sic] improve system performance. (Office Action mailed June 1, 2005, page 7).

It appears that the Examiner believes that merely showing any system having a server coupled between a CMTS and a network is enough to disclose the claimed headend server. In doing so, the Examiner ignores the fact that the headend server, as recited in independent claims 1, 6, 11 and 12, is adapted to handle the problem of non-DOCSIS-compliant data transfer in a cable modem system having a DOCSIS-compliant CMTS. Despite the Examiner's assertions to the contrary, neither Brown nor Fijolek teach or suggest headend servers adapted to handle this problem.

As will be described in detail below, the servers described in Brown are not adapted to handle non-DOCSIS-compliant data transfer, rather they are adapted to control access to a client by intercepting and modifying data traffic transmitted from a network site enroute to the client. Likewise, the server described in Fijolek is not

adapted to handle non-DOCSIS-compliant data transfer, rather it is adapted to balance channel usage by issuing commands through appropriate CMTSs for re-assigning clusters of cable modems to different channels.

I. *Brown does not teach or suggest a specialized headend server for handling non-DOCSIS compliant data transfer from a cable modem to a network in a cable modem system having a DOCSIS-compliant CMTS.*

Brown teaches a method and system that restrict a network site from calling functions in a client set top box (STB), or other form of client. (Brown at col. 2, lines 19-22). Brown fails, however, to teach or suggest a headend server adapted to restore and transfer to a network data packets that have been modified by a cable modem in accordance with a non-DOCSIS-compliant data transfer protocol.

For example, unlike independent claims 1, 6 and 12, which recite a headend server for receiving from a CMTS modified data packets transmitted by a cable modem for transfer to a network, Brown teaches a walled garden proxy server (WGPS) for intercepting messages transmitted from a network site enroute to a client. (*See, e.g.*, Brown at col. 3, lines 4-6, stating that "The WGPS traps messages from the site and determines the ACL for the site."). Nowhere does Brown teach that the WGPS is adapted to receive from a CMTS modified data packets transmitted from the cable modem enroute to the network site.

Furthermore, unlike independent claims 1, 6 and 12, which recite a headend server restoring the contents of data packets modified by a cable modem in accordance with a non-DOCSIS-compliant data transfer protocol, Brown teaches the WGPS modifying the headers of the messages transmitted from the network site by inserting an access control list (ACL). (*See, e.g.*, Brown at col. 3, lines 7-9, stating

that "The WGPS passes the ACL to the client as a header to the message from the site."). Nowhere does Brown teach that the WGPS is adapted to restore the contents of data packets *modified by the cable modem* in accordance with a non-DOCSIS-compliant data transfer protocol.

Moreover, unlike independent claims 1, 6 and 12, which recite a headend server restoring the contents of modified data packets to an unmodified state, Brown teaches the client, not the specialized WGPS, restoring the messages to an unmodified state. (*See, e.g.*, Brown at col. 3, lines 12-13, stating that "The shell executing on the client extracts the ACL from the header when it receives the message.").

In the Abstract, Brown summarizes the system and method as follows:

> The client is in communication with a walled garden proxy server (WGPS), which controls access to a walled garden. The walled garden contains links to one or more servers providing network-based services. The client sends a request to the WGPS to access a service provided by a site in the garden. To provide the service, *the site sends the client a message* containing code calling a function in the API. The *WGPS traps the message from the site* and looks up the site in a table to determine the access control list (ACL) for the site. The ACL is a bit-map that specifies which functions of the client's API can be invoked by code from the site. The *WGPS includes the ACL in the header of the hypertext transport protocol (HTTP) message to the client. The shell receives the message and extracts the ACL.* The shell uses the ACL to determine whether the code has permission to execute any called functions in the API. (Brown at Abstract, emphasis added).

In view of the foregoing, it is clear that the Examiner's assertion that the combination of Chapman and Brown suggests that the operation of restoring suppressed packet headers could be performed at the WGPS cooperating with the CMTS is unfounded. As outlined above, Brown addresses the completely different problem of protecting a client from a network site invoking functions of the client's API without permission, and nowhere does Brown teach or suggest that the WGPS

could be configured to handle non-DOCSIS-compliant data transfer in a cable modem system having a DOCSIS-compliant CMTS.

Since neither Chapman nor Brown, alone or in combination, teaches or suggests all of the limitations of claims 1, 6 and 12, the combination of Chapman and Brown fails to support a prima facie case of obviousness rejection of claims 1, 6, and 12. Furthermore, the combination of Chapman and Brown fails to support a prima facie case of obviousness rejection of claims 3-5, 8-10, 15 and 16 for at least the same reasons as independent claims 1, 6 and 12, from which they depend, and further in view of their own features. Accordingly, the Examiner's rejection of claims 1, 3-6, 8-10, 12, 15 and 16 under 35 U.S.C. § 103(a) is traversed and Applicants respectfully request that the rejection be reconsidered and withdrawn.

II. Fijolek does not teach or suggest a specialized headend server for handling non-DOCSIS compliant data transfer in a cable modem system having a DOCSIS-compliant CMTS.

Fijolek teaches a server 25 having a network administrator 110 that organizes cable modems 16 in clusters to facilitate balancing channel usage by cable modems 16 on a cable system 100. (Fijolek at col. 16, lines 53-57 and col. 17, lines 32-35 and lines 44-46). Fijolek fails, however, to teach or suggest a headend server adapted to restore and transfer to a network data packets that have been modified in accordance with a non-DOCSIS-compliant data transfer protocol.

For example, unlike claim 11, which recites a headend server that receives from a DOCSIS-compliant CMTS data packets modified by a cable modem according to a non-DOCSIS compliant data transfer protocol, Fijolek teaches DOCSIS-compliant CMTSs 12 that receive registration requests from cable modems 16 and

transmit configuration files based on the requests to cable modems 16. (Fijolek at col. 19, lines 28-36). Nowhere does Fijolek indicate that server 25 receives from CMTSs 12 data packets modified by cable modems 16 according to a non-DOCSIS compliant data transfer protocol.

Furthermore, unlike claim 11, which recites a headend server adapted to restore the contents of modified data packets and transfer the restored data packets to a CMTS for forwarding to a network, Fijolek teaches that server 25 is adapted to communicate move commands through appropriate CMTSs 12 to re-assign clusters of cable modems 16 to different channels. (Fijolek at col. 17, lines 53-65). Nowhere does Fijolek indicate that server 25 is adapted to restore the contents of modified data packets and transfer the restored data packets to CMTSs 12 for forwarding to the network.

In view of the foregoing, it is clear that the Examiner's assertion that the combination of Chapman and Fijolek suggests that the operation of restoring suppressed packet headers could be performed at server 25 cooperating with CMTSs 12 is unfounded. As outlined above, Fijolek addresses the completely different problem of balancing channel usage in a cable system, and nowhere does Fijolek teach or suggest that server 25 could be configured to handle non-DOCSIS-compliant data transfer in a cable modem system having DOCSIS-compliant CMTSs.

Since neither Chapman nor Fijolek, alone or in combination, teaches or suggests all of the limitations of claim 11, the combination of Chapman and Fijolek fails to support a prima facie case of obviousness rejection of claim 11. Accordingly,

the Examiner's rejection of claim 11 under 35 U.S.C. § 103(a) is traversed and Applicants respectfully request that the rejection be reconsidered and withdrawn.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Nicole D. Dretar
Attorney for Applicants
Registration No. 54,076

Date: 09-01-2005

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

437498_1.DOC